SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Blockchain Privacy:
An introduction to privacy protocols and their applications for blockchains

In this 2-day course, we will learn about the history of privacy protocols and explore their use in modern-day technologies and blockchain applications.

From communications to commerce, privacy is a fundamental component of our global society and economy. The mathematical discoveries from the last century have been the backbone to securing technologies we use today and the data that gets shared on them.

Blockchains, one of the newest innovations of our time, has seen skyrocketing interest from all over the world; however, it brings with it the risk of not protecting everyday users, as there are no fundamental privacy considerations. Just as HTTPS was a critical component to the mainstream usability of the world-wide web, security protocols that protect users' financial and other transactional data are what will open blockchains to everyday use cases.

Objective

By the end of this course, participants will gain an understanding of:

- The history of cryptographic discoveries and applications
- Privacy protocols built for use in blockchains
- Why zk-SNARKs are the most advanced privacy construction for blockchains today
- The current limitations in SNARKs and future improvements
- The future applications of blockchains enabled with privacy

Topics

Time	Agenda
Day 1	
09:00 – 09:15	2-Day Course Overview
09:15 – 10:45	History: - Historical needs of cryptography - Discoveries in cryptography - Obstacles faced by past cryptographers
10:45 – 11:00	Break
11:00 – 12:30	Cryptography basics: - Privacy vs verification - Digital signatures - Symmetric encryption - Public-key crypto Cryptography applications: - TLS/HTTPS (client/server) - Client-to-client communications - Software verification - Demos of example applications (i.e. Signal)
12:30 – 14:00	Lunch
14:00 – 15:30	Blockchain basics: - Blockchain predecessors - A brief history of blockchains - Use of blockchains
15:30 – 15:45	Break
15:45 – 17:00	Blockchains and cryptography: - Use of cryptographic verification in blockchains - Demo of a client verifying blocks - Use of encryption in blockchains - Demo zcashd
17:00 – 17:30	Assessment
Day 2	
09:00 – 09:15	Overview of the Day
09:15 – 10:45	Introduction: The problem with Bitcoin and other public cryptocurrencies lack of privacy Decoys and mixins as blockchain privacy technologies Some blockchain privacy implementations - MimbleWimble - Monero - Confidential transactions
10:45 – 11:00	Break
11:00 – 12:30	Deeper understanding of zk-SNARKs and Zcash - Zcash as a fork of Bitcoin - zero-knowledge proofs & zk-SNARKs - Transparent vs Shielded addresses - Viewing keys and selective disclosure

12:30 – 14:00	Lunch
14:00 – 17:00	Final points on Zcash Class Exercise: Privacy in blockchain use case proposals
17:00 – 17:30	Assessment

Requirements

- Attendees should have some basic programming skills
- Attendees should have some basic understanding of Bitcoin and blockchain
- Personal laptops will be required – please bring your own

Duration: 2 days

Venue: Singapore University of Social Sciences

Minimum number to run: 25 participants

Certificate of participation is awarded upon 75% attendance for the course

Trainer’s Profile

Zooko is the CEO and Founder of Zcash Company.

Zooko has more than 20 years of experience in open, decentralized systems, cryptography and information security, and startups. He is recognized for his work on DigiCash, Mojo Nation, ZRTP, “Zooko's Triangle,” Tahoe-LAFS, BLAKE2, and SPHINCS. He is also the Founder of Least Authority.

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Course Fee

	Self-sponsored/Company-sponsored				Company-sponsored
	International Participants	**S'poreans and PRs (aged 21 and above)**	**SkillsFuture Mid-Career Enhanced Subsidy[1] (S'poreans aged 40 and above)**	**Workfare Training Support[2] (S'poreans aged 35 and above, and earn ≤ $2,000 per month)**	**Enhanced Training Support for SMEs[3]**
Full course fee (A)	S$1100	S$1100	S$1100	S$1100	S$1100
SSG grant (70%) (B)	-	(S$770)	(S$770)	(S$770)	(S$770)
Nett course fee **(A) - (B) = (C)**	S$1100	S$330	S$330	S$330	S$330
7% GST on nett course fee **(D)**	S$77	S$23.10	S$23.10	S$23.10	S$23.10
Total nett course fee payable, including GST **(C) + (D) = (E)**	S$1177	S$353.10	S$353.10	S$353.10	S$353.10
Less additional funding if eligible under various schemes (F)	-	-	(S$220)	(S$275)	(S$220)
Total nett course fee payable, including GST, after additional funding from the various funding schemes (E) – (F) = (G)	**S$1177**	**S$353.10**	**S$133.10**	**S$78.10**	**S$133.10**

[1] Mid-Career Enhanced Subsidy
Singaporeans aged 40 and above may enjoy subsidies up to 90% of the course fees.

[2] Workfare Training Support
Singaporeans aged 35 and above (13 years and above for Persons With Disabilities) and earn not more than $2,000 per month, may enjoy subsidies up to 95% of the course fees.

[3] Enhanced Training Support for SMEs
SME-sponsored employees (Singaporean Citizens and PRs) aged 21 and above may enjoy subsidies up to 90% of the course fees.

- **Participants are required to achieve at least 75% attendance and/or sit and pass any prescribed examinations /assessments or submit any course/project work (if any) under the course requirement.**
- **The course fees are reviewed annually and may be revised. The University reserves the right to adjust the course fees without prior notice. Singapore University of Social Sciences reserves the right to amend and/or revise the above schedule without prior notice.**

For clarification, please contact the Centre for Continuing and Professional Education (CCPE) via the following:

Telephone: +65 6248 0263
E-mail: CET@suss.edu.sg